FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 1999. március 19-20.

Tűzfaltípusok és alkalmazásai az Interneten

Somlai Gábor

Abstract

The concept of firewall is an effective defending strategy against unauthorized access from the Internet. This brief summary gives an outlined description of the two major types of firewall, namely the packet filtering and the proxy firewalls. The three most common types of proxy firewalls are also included in this short essay without the demand of totality. These pages also contain three sketches of frequently applied firewall topologies, and deals with the desired router configuration in order to improve the local network security.

Bevezetés

Az Internet rohamos fejlődése hamar lehetővé tette mind intézmények, mind magánszemélyek számára a hozzáférést. Így egyre nagyobb rétegnek lett mára létfontosságú a használata, mialatt az Internetes biztonságra is egyre nagyobb súly helyeződött. Egyre több hivatalt ért már támadás távoli gépekről, amelynek következményeként egyre nagyobb összegeket kénytelenek fordítani biztonságosabb hálózati megoldásokra.

A védekezés stratégiaiilag kétféleképpen történhet. Az egyik módszer az, ha minden Internetről elérhető hostot egyenként vétezzünk fel biztonsági elemekkel. Ez hatásos és könnyen áttekinthető megoldás, de csak kis számú hosttal bíró hálózatok esetében. Az intézmények többsége azonban lényegesen nagyobb számítógépparkkal rendelkezik, amely lehetetlenné teszi az efféle stratégia alkalmazását. Kíváncsús tehát egy olyan megoldás, amely egy hálózat összes gépét centralizáltan menedzselni képes, valamint a hálózat minden egyes pontjára egységes biztonságpolitikát tud alkalmazni. Ezen stratégia alapján működnek a tűzfalak (Firewall).

Mi is az a tűzfal?

A tűzfal egy rendszer vagy rendszerek csoportja, amely két hálózat között hozzáférés-ellenőrzési politikát (access control policy) valósít meg. Ez úgy megy végbe, hogy rendelkezik egy szabályhalmazzal, amelynek megfelelően egy beérkező kapcsolatfelvételi kérésről el tudja dönteni, hogy engedélyezhető-e vagy sem. Ha megfelel a szabályoknak, akkor a kapcsolatot felépíti, ellenkező esetben a kérést egyszerűen figyelmen kívül hagyja.

Milyen típusai vannak?

Az Internet protokollja, a TCP/IP réteges felépítésű. A kommunikáció csomagokon keresztül megy végbe, a protokoll egyes rétegei egymás után helyezik a csomagra a fejlécüket. A fejlécek mindenféle, a kommunikációhoz -az adott szinten- elengedhetetlen információkat tartalmaznak, többek között a forrás- és a cél IP címet. Egyfajta csoportosítási lehetőség aszerint adódik, hogy a protokoll mely szintjén monitorozzák az átmenő forgalmat. Így különböztetünk meg *csomagszűrő* és *proxy* tűzfaltípusokat.

Csomagszűrő tűzfalak

Az IP szintjén működik, hálózati szinten monitorozza a csomagokat. A legkisebb kezelt egység a csomag, topológiáját tekintve ez a legegyszerűbb típus. Megvalósítása kétféleképpen lehetséges, hardveres vagy szoftveres úton. Az első esetben a tűzfal tulajdonképpen egy megfelelően konfigurált router, amely csak a hozzáférési listán lévő hostok csomagjait engedi át. Ez a gyakorlatban ma már a hálózatok komplexitása miatt nehezen valósítható meg. A második esetben egy egyszerű számítógép és egy router program alkotja a tűzfalat. A számítógép legalább két hálózati interfésszel rendelkezik: egyvel az Internet és egy másikkal a belső hálózat felé.

Proxy tűzfalak

A csomagszűrő tűzfalakhoz képest magasabb szinten működnek, nem különálló csomagokat, hanem konkrét kapcsolatokat vizsgálnak, ezekre vonatkozólag alkalmazzák a szabályhalmazt. Több fajtájuk van, a Circuit Relay Firewall-ok a szállítási és a viszony réteget szűrik, míg egy kifinomultabb típus az Application Proxy, amely az alkalmazási rétegben működik, és a kapcsolatban végbemenő adatforgalom szűrését is el tudja végezni.

Dual Homed Gateway Firewall

Alapvetően biztonságosabb a csomagszűrő tűzfalaknál. A gateway egy dedikált számítógép, amely két hálózati porttal rendelkezik, és ezen fut a proxy firewall. Az opcionális rész biztonságnövelő tényező, használatával a bekerülő csomagokat vagy csak a proxy, vagy csak az információs szerver felé küldi, és minden egyéb forgalmat letilt.

Screened Host Firewall

A Dual Homed Gateway-nél sokkal rugalmasabb megoldás, bár sokban hasonlít hozzá. A különbség annyiban nyilvánul meg, hogy a gateway csak egy hálózati interfésszel rendelkezik, és a proxy is csak a router által felé engedett csomagokat vizsgálja.

A router a következőképpen van beállítva:

- Az Internet felől érkező csomagok vagy az applikációs gateway-hez, vagy az információs szerver-hez mehetnek.

- Minden egyéb, az Internetről érkező csomag tiltott.
- Belülről kifelé pedig tilt minden csomagot, amelyre van proxy a gateway-en, kivéve magától a gateway-től érkező csomagokat.

Előnye a Dual Homed Gateway-jel szemben, hogy nem kell külön alhálózat a gateway és a router közé, valamint nem kell két hálózati csatlakozó a gateway számára. A hátránya pedig - ami a rugalmasságából is adódik - az, hogy alkalmazási szinten nem ellenőrzött forgalmat is lehetővé tesz az Internet és a belső hálózat között.

Screened Subnet Firewall

Az előző két típus előnyös tulajdonságait ötvözi ez a fajta tűzfal. A két router között egy ún. demilitarizált zóna van. Ez egyfajta köztes terület, amely azt a célt szolgálja, hogy a belső hálózatnak ne legyen közvetlen kapcsolata az Internettel. Az információs szerveren, a mail szerveren és az applikációs gateway-en kívül magában foglalhat egy modem szervert is. Az Interneten lévő router a következőképpen van konfigurálva:

- Az applikációs gateway-től és a mail szervertől az Internet felé a forgalom engedélyezett.
- Applikációs forgalom az Internet felől az applikációs gateway felé és a mail szerver felé engedélyezett.
- Minden más forgalom tiltva van.
- Ezen túlmenően megoldható a routerrel, hogy a belső hálózatra nézve specifikus csomagok (pl. NFS, NIS) ne kerüljenek ki, illetve kívülről ne kerüljenek be. A belső router feladatai a következők:
- Az applikációs gateway és a mail szerver felőli csomagok a belső gépek felé engedélyezettek.
- Az applikációs forgalom a belső gépektől a gateway felé engedélyezett.
- Analóg módon az e-mail forgalom a belső gépektől a mail szerver felé szintén engedélyezett.
- A belső gépektől az információs szerver felé menő forgalom engedélyezett.
- Minden más forgalom tiltott.

A Dual Homed Gateway-hez annyiban hasonlít, hogy egyik belső gép sem érhető el közvetlenül az Internetről és fordítva. A különbség csupán annyi, hogy két router gondoskodik a forgalom irányításáról, ami feleslegessé teszi, hogy a gateway két hálózati interfésszel rendelkezzen. A demilitarizált zónában lévő gépek felkonfigurálhatók olyan módon, hogy a belső gépeket az Internet felé elrejtse, ilyen módon azok nem igényelnek DNS bejegyzést sem.

Somlai Gábor, hallgató, Miskolci Egyetem, Általános Informatikai Tanszék,

E-mail: somlai@iit.uni-miskolc.hu